Design Considerations for a Case-Based Reasoning Engine for Scenario-Based Cyber Incident Notification

Stephen M. Woskov[1], Michael R. Grimaila[1], Robert F. Mills[1], Michael W. Haas[2]

[1]Air Force Institute of Technology / [2]Air Force Research Laboratory
Wright-Patterson Air Force Base, OH, 45433-7765 USA

Abstract—**Virtually all modern organizations have embedded information systems into their core business processes as a means to increase operational efficiency, improve decision making quality, and minimize costs. Unfortunately, this dependence can place an organization's mission at risk if the confidentiality, integrity, or availability of a critical information resource has been lost or degraded. Within the military, this type of incident could ultimately result in serious consequences including physical destruction and loss of life. To reduce the likelihood of this outcome, personnel must be informed about cyber incidents, and their potential consequences, in a timely and relevant manner so that appropriate contingency actions can be taken. In this paper, we identify criteria for improving the relevance of incident notification, propose the use of case-based reasoning (CBR) for contingency decision support, and identify key design considerations for implementing a CBR system used to deliver relevant notification following a cyber incident.**

Keywords-case-based reasoning, relevance, case represenation, case indexing, knowledge acquistion, usability

I. INTRODUCTION

Virtually all modern organizations have embedded information systems into their core business processes as a means to increase operational efficiency, improve decision making quality, reduce response times, exploit automation, and minimize costs [1-2]. However, this dependence can place an organization's mission at risk if the confidentiality, integrity, or availability of a critical information resource has been lost or degraded. Within the military, this type of incident could ultimately result in serious consequences including physical destruction and loss of life. This concern generates the need for personnel to be aware of how cyber incidents affect their organization's mission, so that appropriate contingency actions can be taken. Unfortunately, the current cyber incident notification process within the United States Air Force (USAF) has many limitations [1]. While we have recognized several areas which need improvement, in this paper we focus upon enhancing the *relevance* of incident notification.

We seek to gain a better understanding of relevance and determine a set of criteria that are essential for providing relevant notification. These criteria are used to evaluate current decision support technologies that can be applied to the design of a cyber incident notification system. The primary objective of this research is to contribute to the goals of the Cyber Incident Mission Impact Assessment (CIMIA) program by investigating technologies that can be applied to improve the timeliness and relevance of cyber incident notification [1, 3-4].

This paper is organized in the following manner: Section II describes some fundamental aspects about the military domain that should be considered in a notification system. Section III establishes an understanding of relevance and identifies criteria for providing relevant notification. Section IV synthesizes the findings and presents a list of desired characteristics that a notification system should embody. An evaluation of existing decision support technologies using the criteria revealed that case-based reasoning (CBR) is the most suitable for use in incident notification. Section V provides a background on CBR and finishes by highlighting design areas for initial consideration, which include: case representation, case indexing, knowledge acquisition, and usability. The succeeding sub-sections break out each of these areas in detail. Finally, the paper closes with a conclusion and discussion of future research.

II. MODELING A COMPLEX DOMAIN

Before examining relevance, it is essential to have an understanding about the domain of interest: the military environment. There are some fundamental distinctions between military operations and non-military operations. One of these differences lies in the criticality of decision making. While most organizations experience loss in terms of dollars, poor decision making in the military could result in the loss of life [3, 5]. These severe consequences demand that a cyber incident notification system take into account some key attributes that are intrinsic to military operations.

First, the military environment is dynamic [6-8]. This aspect creates the need to continually update cyber resource dependencies to reflect current operational objectives [3]. Having accurate knowledge about resource dependencies is fundamental for maintaining situational awareness (SA). Endsley [9] defines SA as "knowing what is going on around you" (p. 5). SA has been recognized as a precursor to decision making, and ultimately the performance of actions [9]. Therefore, a cyber incident notification system must have the ability to adapt to the changing military environment to enhance a commander's SA.

Second, warfare is inherently uncertain and unpredictable. This aspect is sometimes called the "fog of war" [6, 10-11]. As a result, military commanders are often limited in the availability and quality of information for decision making. *Joint Publication 3-13* [7] explains that "decisions are made

978-1-4244-9906-9/11/$26.00 ©2011 IEEE

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Design Considerations For A Case-Based Reasoning Engine For Scenario-Based Cyber Incident Notification	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Institute of Technology,Wright-Patterson Air Force Base,OH,45433**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
IEEE Symposium on Computational Intelligence in Cyber Security (CICS), Paris, France, 11-15 April 2011.

14. ABSTRACT
Virtually all modern organizations have embedded information systems into their core business processes as a means to increase operational efficiency, improve decision making quality, and minimize costs. Unfortunately, this dependence can place an organization?s mission at risk if the confidentiality,integrity, or availability of a critical information resource has been lost or degraded. Within the military, this type of incident could ultimately result in serious consequences including physical destruction and loss of life. To reduce the likelihood of this outcome, personnel must be informed about cyber incidents, and their potential consequences, in a timely and relevant manner so that appropriate contingency actions can be taken. In this paper we identify criteria for improving the relevance of incident notification, propose the use of case-based reasoning (CBR) for contingency decision support, and identify key design considerations for implementing a CBR system used to deliver relevant notification following a cyber incident.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**9**	

based on the information available at the time" (p. I-8). Consequently, it is important that a cyber incident notification system can provide benefit to a decision maker even when information is missing, incomplete, or uncertain.

Finally, the complexity in the military environment makes it difficult to develop formal models exclusively using quantitative data. Instead, qualitative methods for the assessment of resource dependencies can be established based on the subjective judgment of knowledgeable individuals. As the environment becomes better understood, quantitative metrics can be added to improve accuracy. To fully capture the domain, all stakeholders should have the ability to provide input. As a result, a cyber incident notification system must make it easy for users to construct and maintain its knowledge base [4].

III. What is Relevance?

With an understanding of the domain established, the concept of relevance is now explored. The study of relevance is most prominent in the field of information science. However, there is no generally accepted meaning [12-14]. A good working definition is articulated by Saracevic [12]: "Relevance is considered as a measure of the effectiveness of a contact between a source and a destination in a communication process" (p. 321). Thus, the goal of this paper can be thought of as improving the *effectiveness* of communicating cyber incidents to decision makers.

In general, all definitions of relevance can be grouped into two main categories, objective and subjective relevance [15]. Objective relevance primarily deals with how well a topic search returns results that deal with that topic. In this view, relevance is dependent upon a query and the search algorithm of the information system being used. Consequently, this concept is also referred to as system-oriented relevance because the role of the user is neglected. In contrast, subjective relevance focuses on how a user perceives the effectiveness of information. Thus, this concept is also referred to as user-oriented relevance [13]. This view has gained more interest due to the realization that end users are the ones who decide whether retrieved information is useful [16]. We believe that this type of relevance is most appropriate toward achieving effective cyber incident notification.

Because subjective relevance is dependent on the user's perspective, it is much harder to determine universal measures. However, there has been some progress toward establishing a core set of determinants. After performing individual studies, Barry and Schamber [17] combined their results to produce a list of ten criteria that were common between their findings: Depth/Scope/Specificity, Accuracy/Validity, Clarity, Currency, Tangibility, Quality of Sources, Accessibility, Availability of Information/Sources of Information, Verification, and Affectiveness. The significance of this research lies in the support of relevance metrics that are important in any context. As a result, these criteria were used as a foundation to identify desired characteristics for improving relevant notification, and subsequently for evaluating different decision support technologies in terms of their ability to improve the relevance of notification.

IV. Notification System Evaluation Criteria

A study of the intended operational environment and the relevance literature were synthesized with the goal of creating a concise list of criteria that a cyber incident notification system should embody. The study yielded seven evaluation criteria that are presented in Table 1. These metrics were used as a means to rank available decision support methodologies and technologies for application in a cyber incident notification system. Among the potential candidates were business process models, enterprise architecture frameworks, CBR, rules-based systems, Bayesian networks, and neural networks.

After a critical review of these methods using the evaluation criteria, it was revealed that CBR is most suitable for providing relevant notification following a cyber incident.

Table 1. Criteria for Providing Relevant Notification

Desired Characteristics	Definition
Adaptable to Environment	Ability of the system to continually provide accurate information over time; flexible to change
Functions with Uncertainty	Ability of the system to provide benefit when decision making information is uncertain or missing
Facilitates Knowledge Acquisition	Ease at which the system allows any user (i.e. domain experts or novices) to enter new knowledge
Low Maintainability	Ease at which the system allows users to maintain the knowledge base
Provides Information Depth	Ability of the system to provide sufficient and focused information to a decision maker (i.e. problem, solutions, additional context)
Presents Information Clearly	Ability of the system to display information in a way that is easy to understand
Provides Tangible Information	Ability of the system to provide definite proven information (i.e. scenarios or hard data)

V. CASE-BASED REASONING

The beginning of CBR can be traced back to the work of Schank and his research on dynamic memory [18-19]. While usually considered as an artificial intelligence topic, CBR also has the interest of cognitive scientists and expert system practitioners [20]. The concept behind CBR is summarized by Riesbeck and Schank [21]: "A case-based reasoner solves new problems by adapting solutions that were used to solve old problems" (Pg. 25). This logic is founded on three underlying assumptions listed by Watson [22]: 1) CBR assumes that the world is regular; what holds true today will most likely be true tomorrow, 2) CBR anticipates that events will repeat because it is the sole reason they are remembered, and finally 3) similar problems have similar solutions.

While commonly labeled as a technology, CBR is actually a methodology for problem solving [23]. Researchers suggest that people cognitively use the concept of CBR on a daily basis [24]. This methodology has been used to develop systems in a number of areas including law, management, health sciences, planning, and technical support [22, 25-28]. There have been various models created to describe the CBR process; however, the most popular one was developed by Aamodt and Plaza [18], as shown in Figure 1.

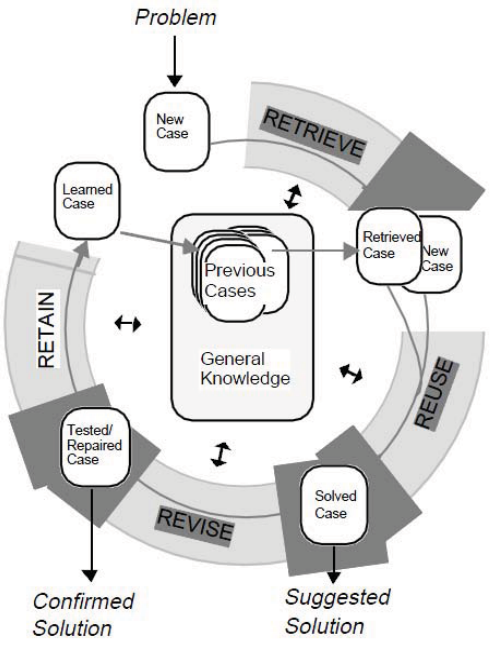

Figure 1. The CBR Cycle [18]

In their cycle, CBR is described by the four REs: RETRIEVE, REUSE, REVISE, and RETAIN. A problem is solved by *retrieving* a past case, *reusing* the previous case in some way, *revising* the solution after using it, and finally *retaining* the new experience in the case-base by either adding the new case or updating existing cases [18]. A unique aspect about CBR is that it relies on specific knowledge from past events, instead of generalized relationships about a specific domain [18]. This ability means that CBR can take advantage of storytelling to improve decision making. Additionally, CBR is an approach that allows for incremental learning. Once a new case is added to its library, it can be retrieved in the future [18]. CBR systems have been particularly useful in domains that are not fully understood [29-30]. Overall, these findings lead us to believe that CBR is a good fit for the complexity found in the military domain.

The benefits of using CBR in a military context have already been recognized. One of the earliest studies in this area was performed by Goodman [31], who developed a decision support aid for battle planning. By taking advantage of an existing database containing historical land battles, this CBR system retrieved past conflicts most similar to a present operation based on user input. In more current research, Jakobson et al. [32] discuss CBR's potential to aid in battlespace management. Their work particularly focuses on the usefulness of CBR within the dynamic environment of military operations. The most similar research to ours was performed by Weber and Aha [33], who used CBR as a framework to design a Lessons Learned System (LLS). Lessons learned are past successes or failures that are pertinent to tasks within an organization. In their work, they combine an LLS with a Decision Support System (DSS) used for military mission planning. While using the DSS, the LLS automatically notifies a user when there is a lesson applicable to the part of the plan that he or she is working on.

This paper builds upon previous studies by focusing on how CBR can be leveraged to provide *relevant* notification of cyber incidents. To achieve this goal, we have identified four key design considerations for applying CBR within a cyber incident notification system: case representation, case indexing, knowledge acquisition, and usability. In the following sub-sections we discuss each of these areas in detail.

A. Case Representation

Before knowledge can be acquired for use within a CBR system, a case representation format should first be determined [34]. Kolodner and Leake [35] define a case as a "contextualized piece of knowledge representing an experience that teaches a lesson fundamental to achieving the goals of the reasoner" (p. 36). The three major parts of a case typically include a problem, a solution, and an outcome [30].

Cases can store knowledge in different ways. For example, CLAVIER was a CBR system designed by Lockheed to aid with the arrangement of composite parts within an autoclave (i.e. a large oven). CLAVIER was able to find past layouts that would allow operators to successfully cure the most high-priority parts at one time [25]. Cases within this system were primarily represented by quantitative attributes such as the relative position of parts, the positions of tables, and production statistics (e.g. start and finish time) [29]. Alternatively, cases can store information in the form of stories. For example, the story producer for interactive learning (SPIEL) worked in conjunction with a simulator to help students learn social skills. By observing the dialogue

between the student and simulator, SPIEL could relate an appropriate past story, in the form of a video (a practitioner speaking from experience), to help educate students on their approaches [36]. It is this qualitative aspect that is missing from the current cyber notification process.

To determine an appropriate case representation format, we must revisit the purpose of our proposed system. Ultimately, we want an improved incident notification process that presents relevant messages to an end user. Our view of relevance shows that it is dependent on the user's perception. From this notion, we believe it is important for users themselves to comment on how certain resources can affect them. More detail about this topic will be covered in the knowledge acquisition section. However, this realization points us toward a new way to look at case representation. In most CBR systems, the solutions provided within a case are limited to one view. While this may be suitable for some domains, our focus on relevance highlights subjectivity. Therefore, cases should be able to provide multiple views and solutions to a problem. Also, most case representations only include the use of text. We believe that adding unit specific mission representation in the form of a picture can further enhance recognition of the relevance of a case upon retrieval.

These ideas can be synthesized into other case representation designs. Again, we draw upon the work by Weber and Aha [33] as a starting point. They use four elements in their case representation for an LLS: 1) *applicable task*, 2) *preconditions*, 3) *lesson suggestion*, and 4) *rationale*. The *applicable task* tells the user when the lesson is appropriate; the *preconditions* show what circumstances must exist for a case to be useful; the *lesson suggestion* offers a possible course of action; and finally the *rationale* shows the user how the lesson was learned. With some modifications, a similar design would provide benefit in our research.

While the LLS was intended to remind a user when information could be useful, our study focuses on creating a warning system. Therefore, we feel that a problem statement is needed to explain why a case is being displayed. We call this field *problem*. It will present an explanation of what is wrong along with a hypertext link to more information if desired.

Next, the *applicable task* element is ideal because it tells users how a problem affects them. However, we believe that capabilities are more enduring than tasks. Thus, we renamed this element and call it *affected capability*. This field can be enhanced by adding a picture. Glenberg and Langston [37] showed that text accompanied by pictures helped individuals build mental models. A diagram like the one proposed in the Risk-to-Mission Assessment Process (RiskMAP) is helpful [38-39] (see Figure 2). This picture can provide a decision maker with a quick snapshot of how an incident at the system level (i.e. network nodes) would impact mission objectives.

Third, the *preconditions* field is important because it shows a user what action or state must be present for a case to be applicable. This knowledge can aid a user in isolating the problem and developing a better understanding about the incident as a whole.

Fourth, the *lesson suggestion* element is needed for providing users with a course of action. However, this field could be improved by including more than one solution. Thus, in our representation we call this component *possible actions*. Multiple stories can provide a richer knowledge base when attempting to make the best decision. However, the user must not be overwhelmed by an abundance of information. For this reason, one action should be listed along with the option to search more that have been submitted by other users. These additional comments can be viewed by accessing a hypertext link to the case-base repository.

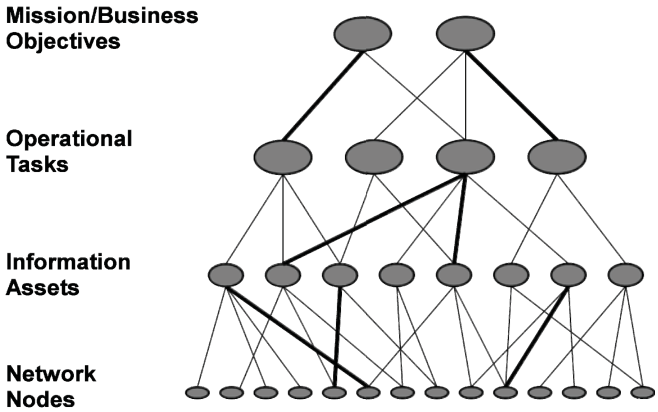

Figure 2. RiskMAP Methodology [39]

Finally, the *rationale* element is significant because it shows the user how the *possible actions* were discovered. This information adds more context to a case and allows the user to have a better understanding about the situation.

To present our case representation design, we will use an example scenario. The Maintenance Operations Center (MOC) is an organization that operates within a maintenance squadron on a USAF installation. The MOC is responsible for helping the squadron ensure aircraft readiness, which is the main mission objective for any maintenance unit [40]. As part of their responsibility, the MOC must enter the readiness status of aircraft into an information system called GO81. These inputs aid higher echelons of command in determining which aircraft are available to perform specific missions. If the GO81 inputs cannot be made, then commanders will not have an accurate list of aircraft that can be tasked. Inability to access GO81 may occur if the Domain Name Server (DNS) was down. Figure 3 shows what this case might look like to a user equipped with a CBR notification system using the five elements previously described: *problem*, *affected capability*, *preconditions*, *possible actions,* and *rationale.*

The *problem* is that the DNS is unavailable, which means that the user is not able to access the GO81 web page by entering the common page name. There is a hypertext link included to educate the user about DNS if he or she is unfamiliar with the term. The *affected capability* is that the user is unable to connect to the World Wide Web. The RiskMAP-like diagram shows how the availability of the DNS server affects the information assets, tasks, and mission. The

preconditions state that this case is only applicable for when a user is attempting to connect to the internet. The *possible actions* show the Internet Protocol (IP) address that can be used to access GO81. There is also a hypertext link that will display other possible actions if the user wants more choices. Finally, the *rationale* adds context to the case by explaining that the internet is not actually down, but only appears to be. This extra information allows the user to be more informed about the problem.

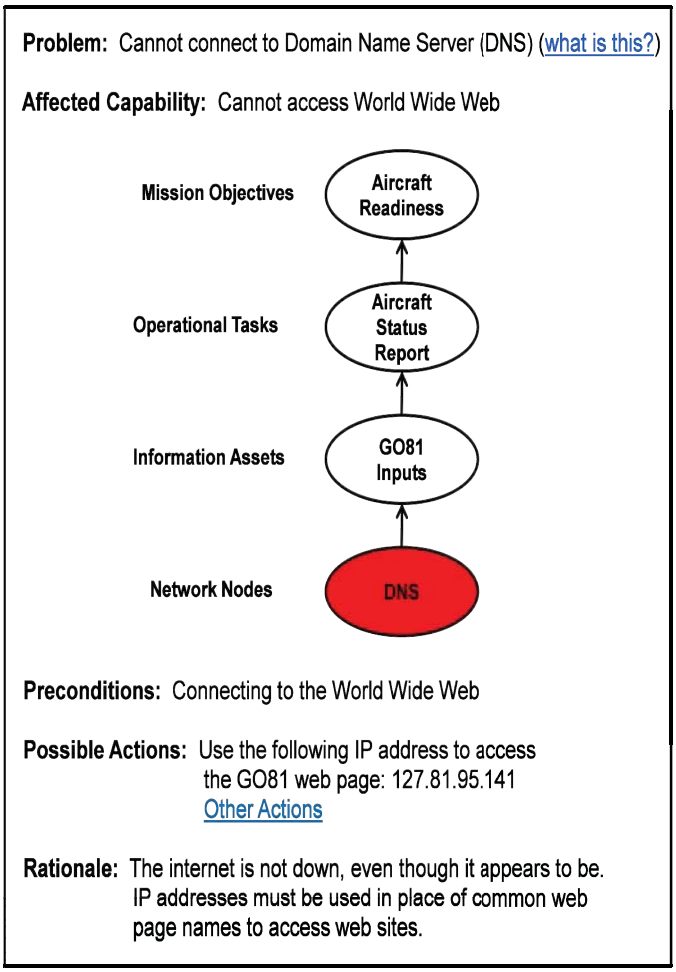

Figure 3. Case Representation for Cyber Incident Notification

B. Case Indexing

Indices are features that represent cases so they can be retrieved quickly [25]. Determining the right indices for cases is commonly referred to as the indexing problem [21, 30]. Kolodner [30] presents four guidelines for creating indices: they should 1) be predicative, 2) address the purpose of the case, 3) be abstract enough for use in multiple situations, and 4) be recognizable. In our research, we believe that the development of indices for our proposed system will be an easier task than for others. This thought stems from the realization that most CBR systems require a user to search for a case. When designing for this type of system, the creation of indices is difficult because the builder must take into account the different search words users may type in when searching for a specific case. In contrast, our proposed notification system will automatically notify users when a case has relevance, much like the LLS [33]. Therefore, the typical user will not need to know how to search for a case.

The user requires notification only when there is a problem with the confidentiality, integrity, or availability (C-I-A) of the information needed from a critical resource. From this notion, the resources become the indices which trigger a case. When all information resources are unaffected by C-I-A, no cases are retrieved. Once a problem arises with a resource, the CBR system will search the library for any cases that match the current situation. This means that the CBR engine must continually check the current state of information resources. It will only act once there is a deviation from the steady state.

The level of index abstraction is crucial within the military environment. As information systems and their connections may change frequently, it is important that indices remain dynamic. Again, we use the DNS as an example. At a detailed level, a DNS could be located via its IP address. However, using the IP address as an index is not appropriate as the address is subject to change. Instead, indices must be stored in a more abstracted representation. Using the example, an index labeled "DNS" would be a better choice because it is suitable for *any* IP address. As a result, this means there must be a separate storage location linking the specific IP address to the DNS.

C. Knowledge Acquisition

The process of acquiring knowledge has been identified as a bottleneck for developing expert systems. Knowledge acquisition processes may involve knowledge engineers, who are people dedicated to collecting knowledge from experts [41]. However, hiring knowledge engineers could be expensive. Puppe and Gappa [42] explain that direct knowledge acquisition is the best approach in terms of cost. The direct method allows experts themselves to formalize their own knowledge and transfer it into an expert system. Additionally, our perspective on the complexity of the military domain suggests the need to capture knowledge directly from the end user. With this support, we believe that direct knowledge acquisition is the most appropriate technique to collect knowledge for a CBR notification system.

However, this method must be addressed carefully. Aha [20] explains that the difficulty of writing cases is a major reason that CBR systems fail in organizations. Therefore, it is essential that users do not feel overwhelmed when creating cases. To avoid this problem, we recommend an incremental case acquisition strategy. In this approach, cases are pieced together over a period of days or weeks.

For this strategy to be successful, we propose the use of automated mapping agents and tutoring techniques to reduce the workload placed on the user. Automated mapping agents can determine the most frequently used resources. For example, a user may connect daily to a specific server outside

his or her unit. When a threshold is reached, the agent will assume that this connection has an important meaning to the user. Now, tutoring principles can be used as the actual method to elicit knowledge about this connection.

Kim and Gil [43] discuss the benefit of including tutoring methods into knowledge acquisition systems. They describe 15 tutoring principles that should be considered. From this research, we find two principles that carry over to our work: 1) generate educated guesses, and 2) indicate a lack of understanding. For the former principle, an agent could ask a user the following: "You [the user] seem to connect to resource A frequently, are you performing an important task?" This dialogue could then be followed up using the latter principle: "How important is this connection to you?" A scale could be included with this message to allow the user to rate the importance level. By using these principles, we believe that knowledge about resource dependencies and their criticality to mission objectives can be established over time.

D. Usability

When new CBR systems are implemented, they may not contain many cases in the case-base. This issue could result in receiving unreasonable solutions from the system, which ultimately prevents users from trusting it. Chan [44] explains that adding rules in the early stages of implementation can help fix this problem. Rules-based reasoning (RBR) systems have higher initial solution accuracy than CBR systems, as shown in Figure 4.

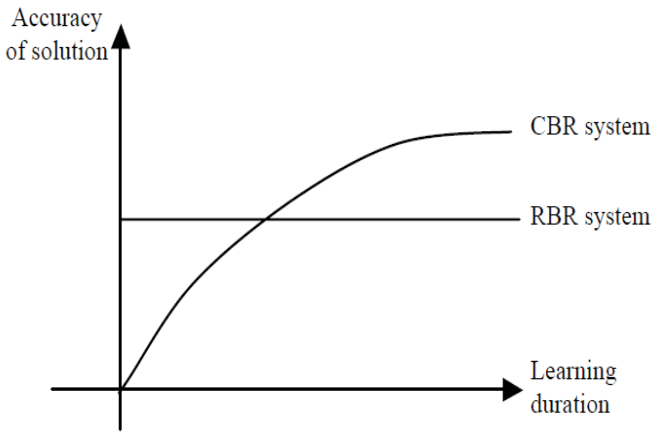

Figure 4. Accuracy of RBR vs. CBR Systems [44]

To increase usability, some rules should be populated into the CBR system during the implementation stages. Once enough cases are added to the case-base, the system will no longer need to rely on rules to provide accurate solutions. Rules take the form of "IF-THEN" statements. To determine an appropriate set of rules, organization members must meet and enumerate the most obvious problems from C-I-A incidents. For example, one possible rule might be "IF the internet is unavailable, THEN GO81 cannot be used for aircraft status reporting."

Many CBR systems have failed due to the lack of user participation, which ceases case library development. In an effort to improve this issue, research by He et al. [45] proposes that the integration of Web 2.0 technology and CBR systems will help encourage users to become more involved with the CBR process. Because problem solving is a social endeavor, they suggest that one reason CBR systems are not broadly accepted is due to the lack of a social environment in current systems [45]. Similar research on the topic of usability is investigating how the design of CBR interfaces can be optimized to encourage acceptance by more users [46]. The users' mental model about how a CBR system searches for information is also important for success. Therefore, a good interface should provide training to help users understand the system [46].

Based on the success of the web page Wikipedia, we believe that its architecture is an ideal framework to use for aiding usability. Cases can be accumulated in a library that has a similar design as Wikipedia. Using this structure would take advantage of consistency, which is one of the key human computer interaction design principles [47]. By maintaining a format that is familiar, users of our proposed CBR notification system may feel more comfortable using it.

VI. CONCLUSION

The current cyber incident notification process within the USAF has several limitations. We have determined one significant area needing improvement: *relevance*. This paper established a list of criteria that are essential for improving relevance. These criteria were used as a means to evaluate decision support technologies for improving incident notification. After a critical review of potential candidates, it was determined that CBR was the most suitable framework. Once selected, initial design considerations were proposed for applying CBR within a cyber incident notification system.

First, a case representation format was designed which displays an incident's impact in the form of a picture. Additionally, the design allows users to view multiple solutions to a problem. Next, it was established that case indices should be stored in an abstracted form so that they can endure a dynamic environment without being changed. Third, a knowledge acquisition strategy was proposed that included gathering information from users in small chunks over time. Finally, some usability aspects were considered, which included adding rules to bootstrap CBR systems during implementation stages and integrating Web 2.0 to increase user participation.

VII. FUTURE WORK

This paper represents the initial research of applying CBR within the cyber incident notification domain. As such, there are some areas that have not been addressed. Uninvestigated CBR topics include retrieval and adaptation. Retrieval focuses on finding cases that most appropriately match the current situation. A reliable retrieval method is needed for a CBR

system to present accurate cases to a user. Adaptation is a process through which cases are altered to help fit a problem more precisely. Including adaptation can enhance the usefulness of a retrieved solution.

Additionally, the proposed system should be scalable along a hierarchical chain. Further investigation on case representation is needed to establish the best method to alert higher headquarters about problems at the lower organizational levels. Finally, while CBR appears to be a feasible methodology to use for cyber incident notification, it must be tested. Future research must build and implement a CBR notification system within an organization.

VIII. Disclaimer

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

References

[1] M. R. Grimaila, G. Schechtman, and R. F. Mills, "Improving cyber incident notification in military operations," in *Proceedings of the 2009 Industrial Engineering Research Conference*, Miami, FL, 2009.

[2] D. L. Pipkin, *Information Security: Protecting the Global Enterprise*. Upper Saddle River, NJ: Prentice-Hall, Inc. , 2000.

[3] M. R. Grimaila, L. W. Fortson, and J. L. Sutton, "Design considerations for a cyber incident mission impact assessment (CIMIA) process," in *Proceedings of the 2009 International Conference on Security and Management*, Las Vegas, NV, 2009.

[4] M. R. Grimaila, L. W. Fortson, J. L. Sutton, and R. F. Mills, "Developing methods for timely and relevant mission impact estimation," in *Proceedings of the 2009 SPIE Defense, Security and Sensing Conference*, Orlando, FL, 2009.

[5] M. R. Grimaila and L. W. Fortson, "Improving the cyber incident damage and mission impact assessment," *IAnewsletter,* vol. 11, pp. 10-15, 2008.

[6] Department of the Air Force, *Air Force Basic Doctrine*. AFDD 1. Washington: HQ USAF, 17 November 2003.

[7] Department of Defense, *Information Operations*. JP 3-13. Washington: United States Department of Defense, Joint Chiefs of Staff, 13 February 2006.

[8] R. R. Leonhard, *The Principles of War for the Information Age*. New York: The Ballantine Publishing Group, 1998.

[9] M. Endsley and D. Garland, Eds., *Situation Awareness: Analysis and Measurement*. Mahwah, NJ: Lawrence Erlbaum Associates, 2000.

[10] C. V. Clausewitz, *On War*. Princeton, NJ: Princeton University Press, 1976.

[11] D. Alberts, J. Garstka, R. Hayes, and D. Signori, *Understanding Information Age Warfare*. Washington D.C.: Command and Control Research Program, 2001.

[12] T. Saracevic, "Relevance: A review of and a framework for the thinking on the notion in information science," *Journal of the American Society for Information Science,* vol. 26, pp. 321-343, 1975.

[13] L. Schamber, M. B. Eisenberg, and M. S. Nilan, "A re-examination of relevance: toward a dynamic, situational definition," *Information processing & management,* vol. 26, pp. 755-776, 1990.

[14] E. Cosijn and P. Ingwersen, "Dimensions of relevance," *Information Processing and Management,* vol. 36, pp. 533-550, 2000.

[15] P. Borlund, "The concept of relevance in IR," *Journal of the American Society for Information Science and Technology,* vol. 54, pp. 913-925, 2003.

[16] C. L. Barry, "User-defined relevance criteria: an exploratory study," *Journal of the American Society for Information Science,* vol. 45, pp. 149-159, 1994.

[17] C. L. Barry and L. Schamber, "Users' criteria for relevance evaluation: A cross-situational comparison," *Information Processing and Management,* vol. 34, pp. 219-236, 1998.

[18] A. Aamodt and E. Plaza, "Case-based reasoning: foundational issues, methodological variations, and system approaches," *AI Communications,* vol. 7, pp. 39-59, 1994.

[19] R. Schank, *Dynamic memory: A theory of reminding and learning in computers and people*. New York: Cambridge University Press 1982.

[20] D. W. Aha, "The omnipresence of case-based reasoning in science and application," *Knowledge-Based Systems,* vol. 11, pp. 261-273, 1998.

[21] C. Riesbeck and R. Schank, *Inside Case-Based Reasoning*. Hillsdale, NJ: Lawrence Erlbaum Associates Inc., 1989.

[22] I. Watson, *Applying Knowledge Management: Techniques for Building Corporate Memories*. San Francisco, CA: Morgan Kaufmann, 2003.

[23] I. Watson, "Case-based reasoning is a methodology not a technology," *Knowledge-Based Systems,* vol. 12, pp. 303-308, 1999.

[24] J. Kolodner, "An introduction to case-based reasoning," *Artificial Intelligence Review,* vol. 6, pp. 3-34, 1992.

[25] I. Watson, *Applying Case-Based Reasoning: Techniques for Enterprise Systems*. San Francisco, CA: Morgan Kaufmann 1997.

[26] K. D. Ashley, "Reasoning with cases and hypotheticals in HYPO," *International Journal of Man-Machine Studies,* vol. 34, pp. 753-796, 1991.

[27] P. Koton, "A medical reasoning program that improves with experience," *Computer Methods and*

Programs in Biomedicine, vol. 30, pp. 177-184, 1988.

[28] K. Hammond, "CHEF: A model of case-based planning," *Proceedings of AAAI-86,* 1986.

[29] D. Hennessy and D. Hinkle, "Applying case-based reasoning to autoclave loading," *IEEE Expert,* vol. 7, pp. 21-26, 1992.

[30] J. Kolodner, *Case-Based Reasoning*. San Mateo, CA: Morgan Kaufmann, 1993.

[31] M. Goodman, "CBR in battle planning," in *Proceedings of the Second Workshop on Case-Based Reasoning*, Pensacola Beach, FL, 1989, pp. 246–269.

[32] G. Jakobson, L. Lewis, J. Buford, and E. Sherman, "Battlespace situation analysis: the dynamic CBR approach," presented at the MILCOM 2004 - 2004 IEEE Military Communications Conference, 2004.

[33] R. O. Weber and D. W. Aha, "Intelligent delivery of military lessons learned," *Decision Support Systems,* vol. 34, pp. 287-304, 2002.

[34] K. Althoff and R. Weber, "Knowledge management in case-based reasoning," *The Knowledge Engineering Review,* vol. 20, pp. 305-310, 2006.

[35] J. Kolodner and D. B. Leake, "A tutorial introduction to case-based reasoning," in *Case-Based Reasoning: Experiences, Lessons, and Future Directions*, D. B. Leake, Ed., ed Menlo Park, CA: AAAI Press/MIT Press, 1996.

[36] R. Burke and A. Kass, "Retrieving stories for case-based teaching," in *Case-Based Reasoning: Experiences, Lessons, and Future Directions*, D. B. Leake, Ed., ed Menlo Park, CA: AAAI Press/MIT Press, 1996.

[37] A. M. Glenberg and W. E. Langston, "Comprehension of illustrated text: pictures help to build mental models," *Journal of Memory and Language,* vol. 31, pp. 129-151, 1992.

[38] P. Kertzner, J. Watters, and D. Bodeau, "Process control system security technical risk assessment methodology & technical implementation," Institute for Information Infrastructure Protection, 2006.

[39] J. Watters, S. Morrissey, D. Bodeau, and S. C. Powers, "The risk-to-mission assessment process (RiskMAP): a sensitivity analysis and an extension to treat confidentiality issues," Institute for Information Infrastructure Protection, 2009.

[40] Department of the Air Force, *Aircraft and Equipment Maintenance Management*. AFI21-101. Washington: HQ USAF, 26 July 2010.

[41] N. M. Cooke and J. E. McDonald, "A formal methodology for acquiring and representing expert knowledge," *Proceedings of the IEEE,* vol. 74, pp. 1422-1430, 1986.

[42] F. Puppe and U. Gappa, "Towards knowledge acquisition by experts," in *Industrial and Engineering Applications of Artificial Intelligence and Expert Systems*. vol. 604, F. Belli and F. Radermacher, Eds., ed: Springer Berlin / Heidelberg, 1992, pp. 546-555.

[43] J. Kim and Y. Gil, "Incorporating tutoring principles into interactive knowledge acquisition," *International Journal of Human-Computer Studies,* vol. 65, pp. 852-872, 2007.

[44] F. T. S. Chan, "Application of a hybrid case-based reasoning approach in electroplating industry," *Expert Systems with Applications,* vol. 29, pp. 121-130, 2005.

[45] W. He, L. D. Xu, T. Means, and P. Wang, "Integrating web 2.0 with the case-based reasoning cycle: a systems approach," *Systems Research and Behavioral Science,* vol. 26, pp. 717-728, 2009.

[46] W. He, F. K. Wang, T. Means, and L. D. Xu, "Insight into interface design of web-based case-based reasoning retrieval systems," *Expert Systems with Applications,* vol. 36, pp. 7280-7287, 2009.

[47] B. Shneiderman and C. Plaisant, *Designing the user interface: strategies for effective human-computer interaction*. Boston: Pearson/Addison Wesley, 2004.